Typed Software Contracts with Intersection and Nondeterminism(Abstract_要旨)

AUTHOR(S):

Nishida, Yuki

様式VI

博士学位論文調査報告書

論 文 題 目

Typed Software Contracts with Intersection and Nondeterminism

交差型と非決定計算を含んだ型付ソフトウェア契約

申請者氏名 西田 雄気

最 終 学 歴　平成２８年　３月

京都大学大学院情報学研究科通信情報システム専攻修士課程　修了

令和　２年　３月

京都大学大学院情報学研究科通信情報システム専攻博士後期課程

研究指導認定退学

学 識 確 認　令和　　年　　月　　日（論文博士のみ）

論文調査委員　京都大学大学院情報学研究科

（調査委員長）　教　授 五十嵐 淳

論文調査委員　京都大学大学院情報学研究科

教　授 山本 章博

論文調査委員　京都大学大学院情報学研究科

教　授 湊 真一

（ 続紙 1 ）

京都大学	博士（情報学）	氏名	西田 雄気
論文題目	Typed Software Contracts with Intersection and Nondeterminism (交差型と非決定計算を含んだ型付ソフトウェア契約)		

（論文内容の要旨）

本論文は，ソフトウェアの仕様記述および検証技法であるソフトウェア契約のための理論を主題としている．ソフトウェア契約は，もともとは，手続きやメソッドの事前条件や事後条件をプログラムの形で表現し，実行時検証に役立てる目的で提案されたが，近年，静的なプログラム検証技術である型システムとの融合が研究されている．本論文は，これまでのソフトウェア契約の枠組みでは表現が難しかった「単純な仕様の列挙によって表現された複合的仕様」の表現，および，そのような複合的仕様を実行時に検査するための技術的課題について理論的側面から研究したものである．論文は全７章から構成されている．

第１章では，研究の背景であるソフトウェア契約および，型システムに契約を統合した型付ソフトウェア契約に関する先行研究が議論された後，本論文で提案されるソフトウェア契約の拡張の概要と技術的貢献が概説されている．

第２章では，単純な型付ソフトウェア契約を取り入れたラムダ計算体系が定義されている．この体系は本論文で提案される拡張を形式化するための基盤となるもので，その型システムは契約検査が必要なところで漏れなく行われることを静的に保証する役割を持ち，操作的意味論はソフトウェア契約に基づく実行時検証アルゴリズムを表現している．章の最後で，型付ソフトウェア契約の計算体系に求められる基本的な性質である型安全性定理が述べられている．

第３章では，第２章の体系に交差型を導入して拡張し，その拡張体系に対して第２章と同様な議論が行われる．交差型は，ひとつのプログラム(断片)が複数の型を同時に持てる場合に与えられる型で，ソフトウェア契約の文脈では，上で述べた、列挙によって表現された複合的仕様に対応している．交差型を導入した体系における契約検査を表現するために，操作的意味論には論理的連言を表現するための組と選言を表現するための非決定性が導入されている．最後に，拡張された型安全性定理が証明されており，交差型を持つプログラムの出力は，それが存在するならば，交差型で結ばれた全てのソフトウェア契約を満足することが示されている．

第４章では，第３章で導入された非決定性とソフトウェア契約の関係がさらに議論されている．まず，素朴に非決定性を導入すると計算体系が矛盾することが議論された後，その問題の解決策として，連係的選択と呼ばれる，一部の非決定的選択が同期するような特殊な非決定的選択演算子が導入される．さらに，第２章の体系を連係的選択演算子で拡張した体系に対する型安全性定理が証明され，プログラムの出力が存在するならば，そのうち少なくともひとつは仕様を満たすことが示される．

第５章では，標準的な非決定的選択演算子が第４章で導入した連係的選択演算子を使って表現できることが，前者を持つ計算体系から後者を持つ計算体系への変換と，その変換が模倣関係であることを証明することで示されている．

最後に，第６章で関連研究について議論がされ，第７章で本論文の結論と今後の方向性が与えられている．

（続紙 ２ ）

（論文審査の結果の要旨）

ソフトウェア契約の概念とソフトウェア契約を備えたプログラミング言語は80年代末に提案されたものだが，2000年代に入ってからは関数型プログラミング言語の文脈で盛んに研究されるようになった．ソフトウェア契約はプログラム検証技術のひとつとして位置づけられるが，もうひとつの代表的なプログラム検証技術である型理論と融合させようという研究が進められてきている．このような研究では，型による静的検査と契約による動的検査をどのように組み合わせればよいかが主な課題となる．本研究は，ソフトウェア契約の表現力を向上させるために型理論で研究されてきた交差型と呼ばれる概念を取り入れ拡張するという研究課題，ならびに，その拡張に付随して発生する理論的な諸問題の解決に取り組んでいる．

本論文で示された成果についての特徴は以下の通りである．

まず，第３章では，ソフトウェア契約の拡張として列挙形式で記述された契約に注目し，そのような契約が記述できるプログラミング言語のモデル(計算体系)を与えた．具体的には，拡張されたソフトウェア契約の実行時検査を計算体系の操作的意味論として与え，その検査手法が妥当であることを，計算体系のメタ定理として証明している．特に，列挙形式の契約の動的検査は，整数などの基本型では簡単だが，関数に対してはどう行えばよいか全く自明ではない．この問題に対し，申請者は複数の検査を同時並行して行うための二種類の機構(すべての検査に通ることを要求するものと，いずれかの検査に通ることを要求するもの)を導入することで解決した．この結果は理論的なもので，実際のプログラミング言語にこの拡張を導入するにはまだ実装上の問題があるが，型理論の観点からは、よく知られた交差型の概念を操作的意味論を使って捉え直した結果として興味深い．

上記の複数の検査を同時並行するための機構のひとつは，言語に非決定性を導入するものと考えられるが，一般に非決定性や入出力などのいわゆる計算効果は型付ソフトウェア契約と相性が悪いことが知られている．第４章では，動的検査の過程だけでなく契約記述にも非決定性を許した場合の問題点と解決策を示している．特に契約と非決定性を素朴に組み合わせるとプログラミング言語がある種の矛盾を来すことを示したことと，それに対して，連係的選択演算子という新しい非決定的選択演算子を導入し，矛盾を防いだことは新規性が高く評価できる点である．

最後に第５章では，この連係的選択演算子の表現力の問題に取り組んでいる．この演算子は，少なくとも表面的には標準的な選択演算子よりも制限が強くプログラミングにおける利便性が低いと思われる．しかしながら，実は，工夫をすることで標準的な選択演算子の振舞いを忠実に模倣できることを証明し，連係的選択演算子の表現力に問題がないことを示した．模倣のためのアイデアは単純だが，証明はエフェクトシステムと呼ばれる型理論の技術を応用しており，かなり技巧的である．

以上のように，本論文は，ソフトウェア契約と型システムというふたつのプログラム検証技術の融合という文脈において，ソフトウェア契約の表現力を強化する提案を行い，その理論的基盤を与えるとともに，そこに派生する問題をプログラミング言語の理論の立場から系統的に解決した研究として意義がある．本論文中の証明は全てCoqという計算機による証明支援システムを使って機械可読な形式で記述されていることも評価できる．

よって，本論文は博士（情報学）の学位論文として価値あるものと認める．また，令和２年４月２０日，論文内容とそれに関連した事項について試問を行った結果，合格と認めた．また，本論文のインターネットでの全文公表についても支障がないことを確認した．

要旨公開可能日：　　年　　月　　日以降